IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI
WESTERN DIVISION

IN THE MATTER OF THE SEIZURE OF ALL FUNDS, INCLUDING VIRTUAL CURRENCIES, IN TARGET ACCOUNT STORED AT PREMISES CONTROLLED BY **NEST SERVICES LIMITED**	Case No. 24-SW-00363-JAM

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, Melanie Wascom, a Special Agent with the Federal Bureau of Investigation being first duly sworn, hereby depose and state as follows:

1. I am employed as a Special Agent with the Federal Bureau of Investigation (hereinafter "FBI"). I have been employed as a Special Agent since August 2023. I am currently assigned to the Kansas City Division, with an investigative focus on White-Collar Crime. As a Special Agent of the FBI, I am authorized to investigate violations of laws of the United States, and I am a law enforcement officer with authority to execute arrest, search, and seizure warrants under the authority of the United States. I have participated in a wide variety of criminal investigations, to include white collar crimes, and other violent and non-violent Federal crimes. Additionally, I have participated in the preparation and/or execution of many search and seizure, and arrest warrants. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(c), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a seizure warrant.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all my knowledge, or the knowledge of others, about this matter.

PURPOSE OF AFFIDAVIT

3. This affidavit is submitted in support of a seizure warrant for the following property, referred to herein as the "**Target Account**" and further described in Attachment A:

a) **Entire contents of Binance Account ID 26687339, an account held by Nest Services Limited.**

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the contents of the **Target Account** constitute or are derived from proceeds obtained, directly or indirectly, from violations of 18 U.S.C. § 1343. There also is probable cause to believe the property described herein was used to conceal the nature, source, ownership, and control of wire fraud proceeds in violation of 18 U.S.C. §§ 1956 and 1957. Accordingly, the contents of the **Target Account** are subject to forfeiture and seizure pursuant to 18 U.S.C. § 981(a)(1)(A) (civil money laundering), 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461 (civil and criminal wire fraud), and 18 U.S.C. § 982(a)(1) (criminal money laundering).

5. Binance confirmed that it had placed a voluntary freeze on the **Target Account** pending a documented official request (i.e. seizure warrant or court order) for the **Target Account** funds.[1]

6. With respect to seizure, 21 U.S.C. § 853(f) provides that a court may issue a criminal seizure warrant when it "determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that a protective order under 21 U.S.C. § 853(e) may not be sufficient to assure the availability of the property for

[1] As explained below, Binance is a cryptocurrency exchange that allows customers to buy, sell, exchange, and transfer a variety of cryptocurrencies. Binance is registered in the Seychelle Islands and, therefore, not subject to U.S. jurisdiction and cannot be compelled by U.S. process. However, as stated, Binance has placed a voluntary freeze on the **Target Account** and is willing to release those assets to U.S. law enforcement authorities upon receipt of a lawful order issued by a U.S. Magistrate Judge.

forfeiture." As set forth further below, there is a substantial risk that the contents of the **Target Account** will be withdrawn, moved, dissipated, or otherwise become unavailable for forfeiture unless immediate steps are taken to secure them at the time the requested searches are executed. As a form of cryptocurrency, some of the funds in the **Target Account** are inherently portable. I therefore submit that a protective order under 21 U.S.C. § 853(e) would not be sufficient to assure that the contents of the **Target Account** will remain available for forfeiture.

7. As set forth below, the **Target Account** includes virtual currencies that (a) are traceable to proceeds of wire fraud and (b) were commingled in the **Target Account** with funds not directly traceable to wire fraud—in an apparent effort to launder the proceeds through the listed **Target Account** as part of concealment money laundering conduct. The **Target Account** is therefore subject to forfeiture because it was involved in apparent concealment money laundering conduct. *See, e.g.*, *United States v. Guerrero*, 2021 WL 2550154, *9 (N.D. Ill. June 22, 2021) (money from unknown source that was commingled with fraud proceeds facilitated the concealment laundering of the fraud proceeds and, accordingly, property acquired with the commingled funds was forfeitable as property traceable to property involved in a money laundering offense); *United States v. Romano*, 2021 WL 1711633, *5-6 (E.D.N.Y. Apr. 29, 2021) (by laundering fraud proceeds through their personal bank accounts, to commingle the proceeds with other funds for a concealment laundering purpose, the defendants made the commingled funds forfeitable as facilitating property); *United States v. Coffman*, 859 F. Supp. 2d 871, 876-77 (E.D. Ky. 2012) (holding that forfeiture of legitimate and criminal proceeds commingled in an account is proper as long as the government demonstrates that the defendant pooled the funds to facilitate money laundering by, for example, disguising the nature and source of proceeds; concluding that clean funds in bank account were subject to forfeiture because they had "been

co[m]mingled with tainted funds for the purpose of obfuscating the origin or existence of the tainted money").

8. For the reasons listed above, the United States seeks combined criminal and civil seizure warrants, authorizing law enforcement to seize the **Target Account** and preserve its contents pending further forfeiture proceedings.

BACKGROUND REGARDING VIRTUAL CURRENCIES AND VIRTUAL CURRENCY EXCHANGES

9. Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies such as the United States Dollar, but rather are generated and controlled through computer software. Bitcoin is currently one of the most popular virtual currencies in use.

10. Virtual currency addresses are the digital locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of letters and numbers.

11. Virtual currency exchanges, like Binance, are trading and/or storage platforms for virtual currencies, such as Bitcoin. Many exchanges also store their customers' virtual currency in virtual currency accounts. These virtual currency accounts are commonly referred to as wallets and can hold multiple virtual currency addresses.

12. Many virtual currencies, including Bitcoin, publicly record all their transactions on what is known as a blockchain. The blockchain is a distributed public ledger containing an immutable and historical record of every transaction utilizing that blockchain's technology.

13. Blockchain explorers are online tools that operate as a blockchain search engine allowing users the ability to search for and review transactional data for any addresses on a

particular blockchain. The blockchain explorer uses a database to arrange and present the data to a user in a searchable format.

FACTS SUPPORTING PROBABLE CAUSE

A. Overview of Criminal Activity

14. On July 10, 2024, an individual referred to herein as "Victim 1," who resides in Platte County, Missouri, received a text message that appeared to be from Victim 1's insurance company. The text message included a hyperlink. Victim 1 clicked on the hyperlink and began an online conversation with an individual named "Richard" who claimed to be an insurance agent. Richard asked Victim 1 to pay Victim 1's insurance coverage. Richard instructed Victim 1 how to pay. Victim 1 withdrew cash from the bank and took the money to a Bitcoin-based automated teller machine ("BTM") operated by Bitcoin Depot. Bitcoin Depot operates BTMs where individuals can convert fiat currency (general government currency like dollars, Euros, or pounds) into cryptocurrency. Victim 1 transferred Bitcoin to the individual he believed to be Richard to pay for insurance.

15. In my training and experience, I know that foreign groups and individuals targeting Americans in fraud and scam schemes commonly ask their victims to exchange their personal U.S. currency into cryptocurrency using Bitcoin BTMs. Many BTMs do not require photo identification to conduct transactions ranging from $250 to over $1,000. BTMs also are ubiquitous in major metropolitan areas, like Kansas City, and do not require users to navigate complex online trading platforms. The BTMs also do not require third-party verification, which allows for quicker transfers than wire transfers through traditional financial institutions and also permits users to exceed daily deposit limits by using BTMs controlled by different operators. The number, accessibility and speed of these BTMs, combined with the lack of verification standards, makes it

easier for illicit actors to launder and steal funds from unsuspecting victims who may possess little to no prior experience with cryptocurrency. Furthermore, all BTMs charge a certain percentage of the transaction fee from the transfer amount. The amount, typically between 7% and 20%, is far greater than fees charged to transfer funds by traditional financial institutions.

B. Tracing Illicitly Obtained Funds from Victim 1 to the Target Account

16. Victim 1 provided two receipts from the Bitcoin Depot BTM to the Platte County, Missouri Sheriff's Office. The first receipt showed a purchase of 0.06080055 Bitcoin on July 11, 2024, at approximately 12:22pm CDT, which was transferred to wallet address bc1q0xtkr9vxtarcne7kfelvds7xhmympqjqjf5h9. The second transfer was on July 11, 2024, at approximately 6:53pm CDT. The second receipt did not show the amount transferred in Bitcoin, but the receipt showed that Victim 1 paid $20,000 in cash to purchase Bitcoin and transferred it to the same wallet address. The Platte County Sheriff's Office used open-source block chain analysis to determine that there was also a third Bitcoin transfer made by Victim 1 to the wallet address above. According to records obtained from Bitcoin Depot, Victim 1 sent a total of approximately 0.5512 Bitcoin, which cost $45,000, including Bitcoin Depot BTM transaction fees, to this wallet address. Soon after, the illicit proceeds from Victim 1 were transferred directly from the wallet to Binance account 26687339 (the **Target Account**).

17. In furtherance of the investigation into the whereabouts of the illicit proceeds referenced herein, on July 25, 2024, the Platte County Sheriff's Office requested "Know Your Customer" information from Binance for the customer account that received the illicit proceeds. On July 26, 2024, Binance provided the following information for the **Target Account**:

a. User ID: 26687339

b. Email: nikhil2404@icloud.com

c. Name: Nikhil Agarwal

d. Created On: February 19, 2018

18. An analysis of the IP addresses used to access the **Target Account** revealed that the account was primarily accessed using IP addresses that geolocate to Kolkata, India. According to Binance, Agarwal provided an Indian identification card with the number 804617257598, and Agarwal's date of birth is January 1, 1997. The phone number associated with the account is +97688014343. The phone number has a country code +91, which is the country code of India.

19. Between July 10, 2024, and July 12, 2024, Agarwal exchanged through Binance the 0.5512 Bitcoin held in the **Target Account**, which was received from Victim 1, for approximately 31,791.47 Tether.[2] On July 15, 2024, Agarwal transferred 39,000 Tether to the address TK9XbdHKRErBn3VteHNTu4qexRxweYhqp3. The address is associated with the Tron Network, which is a decentralized, blockchain-based operating system.

C. Tracing Funds from Other Potential Victims to the Target Account

20. On May 6, 2023, the **Target Account** received approximately 0.1947 Bitcoin from the source address bc1q0wu0tqp2u3rtunjl0h0rsl9pvf86acy6sep63st0lp7lgg67ykzqeq89pn. According to open-source block chain analysis, the source address is affiliated with Bitcoin Depot. In other words, as with the funds paid by Victim 1, the 0.1947 BTC was transferred to the **Target Account** from a Bitcoin BTM. A few minutes later, Agarwal exchanged 0.1946 Bitcoin for

[2] "Tether" (which is traded under the "USDT" symbol) is a blockchain-based cryptocurrency whose tokens in circulation are backed by an equivalent amount of U.S. dollars, making it a stablecoin with a price pegged to USD $1.00.

approximately 5,741.79 Tether.[3] After the exchange, Agarwal transferred 5,567 Tether from the **Target Account** to the address TRPfCtBYU8N9JW23xrkbcPe8V3mAZR3jfq.

21. On May 9, 2023, the **Target Account** received approximately 0.2724 Bitcoin from the source address 3HVn6LtjLUCTEk6EfG9sCzJD6B9W3xkMqi. According to open-source block chain analysis, the source address was affiliated with CoinHub. CoinHub operates BTMs where virtual currency can be purchased. A few minutes later, Agarwal exchanged approximately 0.2724 Bitcoin for approximately 7,537.53 Tether. On May 10, 2023, Agarwal made two transfers from the **Target Account**. The first transfer was for approximately 405 Tether to the address TM7XE6zh9EmauvTLgfDhh7MjfwxcqfgmwR, and the second transfer was for approximately 7,100 Tether to the address TRcWMhyjkyEyAvkKgmoRfdwwz646KgaFGf.

22. On June 29, 2023, the **Target Account** received approximately 0.2734 Bitcoin from the source address bc1q0wu0tqp2u3rtunjl0h0rsl9pvf86acy6sep63st0lp7lgg67ykzqeq89pn. According to open-source block chain analysis, the source address was affiliated with Bitcoin Depot. A couple of minutes later, Agarwal exchanged 0.2734 Bitcoin for approximately 8,221.96 Tether. After the exchange, Agarwal transferred 8,319 Tether from the **Target Account** to the address TRPfCtBYU8N9JW23xrkbcPe8V3mAZR3jfq.

23. Bitcoin Depot BTMs are only located in the United States of America and Canada and Coinhub BTMs are only known to be located in the United States. Because Agarwal is located in India, there is probable cause to believe there are other victims not yet identified whose funds were stolen by Agarwal following the same pattern as Victim 1.

D. Use of Target Account to Facilitate Money Laundering

[3] The discrepancy between the 0.1947 BTC transferred into the Target Account and the 0.1946 BTC subsequently exchanged for Tether may be explained by Binance's 0.1% standard trading fee.

24. The evidence gathered thus far establishes probable cause to believe that the **Target Account** was utilized as a "funnel account" to conceal and lander illicit funds; specifically, criminal proceeds from an international cryptocurrency scam in which Agarwal fraudulently induced victims to buy and transfer cryptocurrency by impersonating legitimate businesses.

25. As of August 5, 2024, the **Target Account** contains the equivalent of approximately 7.76743 Bitcoin valued at approximately $421,585.01.

26. In my training and experience, actors who illicitly use virtual currency know that most virtual currency blockchains are public and can be traced by law enforcement and others using blockchain analytics tools. Therefore, these criminal actors do their best to launder their criminal proceeds through a variety of means, including shuffling the virtual currency through numerous addresses before being transferred to an offshore virtual currency exchange.

27. In doing so, not only can criminal actors transfer criminal proceeds incredibly fast between cryptocurrency addresses, but they can also commingle those proceeds with other funds in order to thwart attempts at tracing the origin and destination by law enforcement. In addition, the criminal proceeds, whether mixed with other funds or not, can be converted into another cryptocurrency; such as in this case, Bitcoin to Tether. All of this was done in this matter: funds were converted into multiple different types of cryptocurrencies, moved through multiple exchange accounts, and were comingled with funds of unknown origins from multiple other sources. In my training and experience, this was done to obfuscate the source and destination of the funds in question and thereby thwart law enforcement's ability to trace and track victim funds.

28. Based on the information discussed above and my observations, I believe the **Target Account** has been used to facilitate the laundering of proceeds traceable to a scam and

fraud scheme perpetrated by Agarwal against individuals in the Unites States. In addition, the rapid movement of the money is not consistent with typical business or personal transactions.

29. The above virtual currency tracing has shown that at least a portion of the illicitly obtained Bitcoin was laundered through multiple virtual currency addresses, including the **Target Account**. The government seeks the seizure of the **Target Account** as property that facilitated money laundering by Agarwal with the purpose of obfuscating the origin of the criminal proceeds.

Fungibility

30. One civil theory of forfeiture allows the Government to forfeit funds on deposit in an account where, within the last year, funds subject to forfeiture have been deposited, without identifying the specific property involved in the offense. In pertinent part, 18 U.S.C. § 984(a) provides:

> (1) In any forfeiture action in rem in which the subject property is cash or funds deposited in an account in a financial institution;
>
> (A) it shall not be necessary for the Government to identify the specific property involved in the offense that is the basis for the forfeiture; and
>
> (B) it shall not be a defense that the property involved in such an offense has been removed and replaced by identical property.

31. Therefore, except as to actions against funds held in an interbank account (which is not the case here), any identical property found in the same place or account as the property involved in the offense that is the basis for the forfeiture shall be subject to forfeiture under this section. *See United States v. $8,221,877.16*, 330 F.3d 141, 158 (3d Cir. 2003) ("Section 984 is a 'substitute asset provision' enacted to overcome ... tracing difficulties and ease the government's burden of proof in civil forfeiture proceedings involving fungible property.") Put more simply,

Section 984 allows the United States to seize for civil forfeiture identical property found in the same place where the "guilty" property had been kept. *United States v. All Funds Distributed To, or o/b/o Weiss*, 345 F.3d 49, 59 n.13 (2d Cir. 2003).

32. I am advised that, by Section 984(a)(1)(B), therefore, this affidavit need not demonstrate that the monies now in the **Target Account** are the particular monies involved in the wire fraud against Victim 1, so long as the forfeiture is sought for other funds on deposit in that account. Although, for the reasons explained above, there is probable cause to seize their entire contents of the **Target Account** on a money laundering theory, the Government is entitled to at least the identical amount of funds stolen from Victim 1 that were moved through the **Target Account**, or 0.5512 Bitcoin.

CONCLUSION

33. The evidence gathered thus far establishes probable cause to believe the **Target Account** was utilized as part of a scheme to defraud Victim 1 of approximately $45,000 by wire fraud, in violation of 18 U.S.C § 1343. Based on these crimes, approximately 0.5512 Bitcoin received by the **Target Account** are subject to seizure and forfeiture pursuant to 18 U.S.C §§ 981(a)(1)(C) and 984, 21 U.S.C. § 853(a) and (f), and 28 U.S.C. § 2461(c).

34. Additionally, based upon the foregoing, probable cause exists to believe that the contents of the **Target Account** constitute property involved in transactions in violation of 18 U.S.C. §§ 1956 and 1957, and therefore, the entire contents of the account are subject to seizure and forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1), 21 U.S.C. § 853(e) and (f), and 18 U.S.C. § 982(b)(1). Accordingly, the application for seizure warrant requests seizure of the entire contents of the **Target Account**.

FURTHER AFFIANT SAYETH NAUGHT.

Melanie Wascom
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me via telephone or other reliable electronic means on this

8th day of August 2024. At 3:32 pm with signatures confirmed telephonically

HONORABLE JILL A. MORRIS
United States Magistrate Judge
Western District of Missouri

ATTACHMENT A

I. Seizure Procedure

The United States is authorized to seize the full account balance in the **Target Account** by having the Subject Provider transfer all funds in the **Target Account** to a United States-controlled virtual currency wallet specified by the government.

II. Subject Provider

Nest Services Limited

House of Francis, Room 303, Ile Du Port, Mahe, Seychelles

III. Target Account

User ID	Name	Email Address
26687339	Nikhil Agarwal	Nikhil2404@icloud.com